AMENDED

April 30, 2014

**H. 4791**

Introduced by Reps. G.R. Smith, Rutherford, Bedingfield, Atwater, Putnam, Southard, Knight, Jefferson, Bowers, J.R. Smith, Hamilton, Bingham, McCoy, Willis, Quinn, Newton, Norrell, Bannister, Burns, Chumley, Delleney, Forrester, Harrell, Henderson, Hixon, Kennedy, Loftis, Lowe, Lucas, V.S. Moss, Owens, Pitts, Sandifer, Simrill, G.M. Smith, Stringer, White, Whitmire, Williams and Wood

S. Printed 4/30/14--H.

Read the first time February 26, 2014.

**A** **BILL**

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, TO ENACT THE “ELECTRONIC DATA PRIVACY PROTECTION ACT” BY ADDING CHAPTER 53 TO TITLE 23, SO AS TO PROVIDE THAT AN ENTITY MAY NOT SEARCH AN ELECTRONIC DEVICE WITHOUT A SEARCH WARRANT, TO PROVIDE EXCEPTIONS, AND TO PROVIDE CERTAIN NOTICE REQUIREMENTS.

Amend Title To Conform

Be it enacted by the General Assembly of the State of South Carolina:

SECTION 1. Title 23 of the 1976 Code is amended by adding:

“CHAPTER 53

Electronic Data Privacy Protection Act

Section 23‑53‑10. This chapter may be cited as the ‘Electronic Data Privacy Protection Act’.

Section 23‑53‑20. The purpose of this chapter is to clarify requirements for searches of electronic messages, mobile devices incident to arrest, and obtaining geolocation information.

Section 23‑53‑30. As used in this chapter, unless the context clearly indicates otherwise:

(1) ‘Electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, photooptical system, or any other device that affects intrastate, interstate, or foreign commerce, but does not include:

(a) any wire or oral communication;

(b) any communication made through a tone‑only paging device; or

(c) any communication from an electronic or mechanical device, except a cell phone, which permits the tracking of the movement of a person or an object.

(2) ‘Electronic communication service’ means a service that provides to users the ability to send or receive wire or electronic communications.

(3) ‘Electronic device’ means a device that contains electronic data; or enables access to, or use of, an electronic communication service, remote computing service, or geolocation information service; or a radio‑frequency identification chip or other transponder.

(4) ‘Electronic storage’ means any storage of electronic data on a computer, computer network, or computer system, regardless of whether the data is subject to recall, further manipulation, deletion, or transmission, and includes any storage or electronic communication by an electronic communications service or a remote computing service, as well as temporary intermediate storage of electronic data or information incidental to the electronic transmission of electronic data or communication.

(5) ‘Electronic data’ means data or records that are in the possession, care, custody, or control of a provider of an electronic communications service, a remote computing service, or geolocation information service, that contains:

(a) information revealing the identity of the owner, operator, or subscriber of the applicable service, device, or program;

(b) information about the owner’s, operator’s, or subscriber’s use of the applicable service, device, or program;

(c) information that identifies the recipient or destination of an electronic communication sent to or by the owner, operator, or subscriber;

(d) the content of an electronic communication sent to or by the owner, operator, or subscriber; or

(e) any data, documents, files, or communications stored by or on behalf of the owner, operator, or subscriber with the applicable service provider or on the owner’s, operator’s, or subscriber’s electronic device.

(6) ‘Geolocation information’ means any information that is not the content of a communication concerning the location of an electronic device that, in whole or in part, is generated by or derived from the operation or tracking of that device and that could be used to determine or infer information regarding the location of the person, but does not include Internet protocol addresses.

(7) ‘Geolocation information service’ means the provision of a global positioning service or other mapping, locational, or directional information service to the public, or to such class of users as to be effectively available to the public, by or through the operation of any wireless communication device, including any electronic device, global positioning system receiving device, or other similar or successor device.

(8) ‘Governmental entity’ means the State or any of its political subdivisions, including school districts.

(9) ‘Remote computing service’ means, as defined in 18 U.S.C. Section 2711(2), the provision to the public of computer storage or processing services by means of an electronic communications system, as defined in 18 U.S.C. Section 2510(14).

(10) ‘Vulnerable adult’ means a person eighteen years of age or older who has a physical or mental condition which substantially impairs the person from adequately providing for his or her own care or protection. This includes a person who is impaired in the ability to adequately provide for the person’s own care or protection because of the infirmities of aging including, but not limited to, organic brain damage, advanced age, and physical, mental, or emotional dysfunction. A resident of an operated or contracted facility, as defined in Section 43‑35‑10, is a vulnerable adult.

Section 23‑53‑40. (A) Except as provided in this chapter or another provision of law, a governmental entity may not conduct a search of an electronic device in the possession of an individual incident to a lawful custodial arrest without a valid search warrant or court order issued by a duly authorized judge or justice using state warrant procedures and based upon probable cause or without a court order issued by a duly authorized judge or justice based upon probable cause, except:

(1) with the consent of the owner, operator, or subscriber of the electronic device;

(2) in exigent circumstances that would cause a reasonable person to believe that a search is necessary to prevent physical harm to the officers or other persons, the destruction of evidence, or the escape of a suspect; or

(3) when the electronic device has been abandoned by the owner, operator, or subscriber.

(B) If an electronic device is searched pursuant to subsection (A)(2), the law enforcement agency shall notify a court of record of the search within two business days of the search being performed.

(C) A governmental entity may not obtain geolocation information revealing the past, present, or future location of an electronic device except:

(1) with a valid search warrant or court order issued by a duly authorized judge or justice using state warrant procedures and based upon probable cause or with a court order issued by a duly authorized judge or justice based upon probable cause;

(2) with the consent of a parent or legal guardian of a minor, vulnerable adult, or person adjudicated to be mentally incompetent to whom the geolocation information pertains;

(3) when such geolocation information is accessed through a system that is configured so that such information is readily accessible to the general public; or

(4) when such geolocation information is accessed because of exigent circumstances that would cause a reasonable person to believe that a such information is necessary to prevent physical harm to the officers or other persons or the escape of a suspect;

(5) to locate a stolen electronic device with the consent of the owner, operator, or subscriber of such device; or

(6) in an emergency, if the geolocation information is used to respond to a request for assistance from the person to whom the information pertains.

(D) If a law enforcement agency obtains geolocation information pursuant to subsection (C)(4), the law enforcement agency shall notify a court of record of the information being obtained within two business days, unless the court orders otherwise.

(E)(1) A search warrant, order from a court of record, or a subpoena may be issued for electronic data, including the contents of and records and other information related to electronic communication held in electronic storage, by a provider of an electronic communications service or a provider of a remote computing service regardless of whether the owner’s, operator’s, or subscriber’s data is held at a location in this State or at a location in another state.

(2) A search warrant, order from a court of record, or a subpoena issued pursuant to this chapter may be served only on a service provider that is a domestic entity or a company or entity otherwise doing business in the United States under a contract or terms of service agreement with a resident of the United States, if any part of that contract or agreement is to be performed in this State, and the service provider shall produce all information sought regardless of where the information is held and within the period allowed for by law for compliance with the warrant or the order from the court of record.

(F)(1) A governmental entity may not compel an electronic communication service or remote computing service to disclose the content of a user’s communications without a valid search warrant or court order issued by a duly authorized judge or justice using state warrant procedures and based upon probable cause or without a court order issued by a duly authorized judge or justice based upon probable cause.

(2) Notwithstanding item (1), an electronic communication service or remote computing service may disclose the content of a user’s communications to a governmental entity:

(a) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(b) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(c) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(d) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(e) to the National Center for Missing and Exploited Children, in connection with a report submitted pursuant to 18 U.S.C. Section 2258A;

(f) to a law enforcement agency, if the contents:

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; and

(g) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

Section 23‑53‑60. (A) Nothing in this chapter shall be interpreted to affect the rights and responsibilities of providers of an electronic communication service, geolocation information service, remote computing service, or a governmental entity conferred by 18 U.S.C. Section 2702 (a)‑(c), 47 U.S.C. Section 222, or a lawful exception to the warrant requirement.

(B) A provider of geolocation information service, electronic communication service, or remote computing services may divulge geolocation information pertaining to the owner, operator, or subscriber of such service to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of geolocation information relating to the emergency.

(C) No later than two business days after seeking disclosure of information pursuant to subsection (B), the governmental entity seeking to conduct the search or obtain the geolocation information shall file with the appropriate court a written statement setting forth the facts giving rise to the emergency and the facts as to why the information sought is believed to be important in addressing the emergency.

Section 23‑53‑70. No cause of action shall lie in any court of this State against any provider of an electronic communications service, remote computing service, or geolocation information service, or its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a warrant, order from a court of record or subpoena, or exception pursuant to this chapter.

Section 23‑53‑80. An original or certified copy of electronic data produced pursuant to a warrant or exception in accordance with this chapter shall be self‑authenticating and admissible into evidence as provided.

Section 23‑53‑90. The South Carolina Law Enforcement Division shall promulgate regulations pursuant to this chapter so as to provide uniform guidelines and training programs for law enforcement agencies that perform searches of electronic messages or mobile devices incident to arrest, and that obtain geolocation information. Law enforcement agencies that perform searches of electronic messages or mobile devices incident to arrest, and that obtain geolocation information shall use the regulations developed by the Criminal Justice Academy to provide written guidelines and to provide training programs for its officers and employees regarding the requirements for searches of electronic messages, mobile devices incident to arrest, and obtaining geolocation information.

Section 23‑53‑100. (A) Nothing in this chapter shall be interpreted or construed to pertain to the use of electronic monitoring devices that are pursuant to conditions of bond, home detention, probation, parole, being categorized as a sex offender, or any other court ordered or statutory mandate.

(B) Nothing in this chapter shall restrict or limit agents of the Department of Corrections, Department of Juvenile Justice, and Department of Probation, Parole and Pardon Services from the authority to conduct searches of electronic devices and receive electronic data from electronic communication services for offenders under supervision.

(C) The provisions of this chapter shall not apply to a government entity’s search of electronic devices determined to be contraband pursuant to Section 24‑3‑950.”

SECTION 2. The repeal or amendment by this act of any law, whether temporary or permanent or civil or criminal, does not affect pending actions, rights, duties, or liabilities founded thereon, or alter, discharge, release or extinguish any penalty, forfeiture, or liability incurred under the repealed or amended law, unless the repealed or amended provision shall so expressly provide. After the effective date of this act, all laws repealed or amended by this act must be taken and treated as remaining in full force and effect for the purpose of sustaining any pending or vested right, civil action, special proceeding, criminal prosecution, or appeal existing as of the effective date of this act, and for the enforcement of rights, duties, penalties, forfeitures, and liabilities as they stood under the repealed or amended laws.

SECTION 3. This act takes effect upon approval by the Governor.

‑‑‑‑XX‑‑‑‑